UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. CIAN BURLEY, Defendant.	Case No. 21-cr-00198-EMC-1 **ORDER GRANTING MICROSOFT'S MOTION TO QUASH** Docket No. 73

I. INTRODUCTION

Defendant Cian Burley served on third party Microsoft a subpoena *duces tecum* pursuant to Federal Rule of Criminal Procedure 17(c). Docket No 73-1 Ex. A (subpoena); Fed. R. Crim. P. 17(c). Microsoft and Defendant have resolved nine of Defendant's requests, and two requests remain outstanding: Defendant's fifth and tenth requests. Docket No. 73 (Mot. to Quash Reqs. ("Mot.")) at 1. Request 5 now seeks "training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography files, and classification standards of suspected child pornography in effect around the time of CyberTip 52016239, from July 5, 2019, [suspected CP first flagged] until August 7, 2019 [date when NCMEC processed the CyberTip]." Mot. at 6. Request 10, in relevant part, now seeks "policies, reports, guidelines, and manuals that set forth the procedures for review, and reporting of accounts containing suspected child pornography files, whether manual or automated . . . from July 5, 2019, [suspected CP first scanned] until August 7, 2019 [NCMEC date processed]." *Id.* Microsoft moves to quash Request 5 and the above section of Request 10 as insufficiently specific, irrelevant, inadmissible, and unduly burdensome. Mot. at 7-16. Having considered the parties' briefs and accompanying submissions, as well as the oral argument of counsel, the Court hereby **GRANTS** Microsoft's motion to quash.

II. BACKGROUND

On July 5, 2019, Microsoft detected four images of child sexual abuse and exploitation allegedly uploaded by Defendant to Skype. *Id.* at 3. Microsoft filed a CyberTip with the National Center for Missing and Exploited Children ("NCMEC"), which NCMEC received on July 9, 2019, and then forwarded to law enforcement. *Id.*; Docket No. 73-1 Ex. C (CyberTipLine Report). After police personnel viewed the files, the U.S. government filed a complaint against Defendant Burley on February 9, 2021, in which they charged Defendant with the possession and distribution of child pornography. Docket No. 1; Docket No. 79 (Def.'s Opp'n to Microsoft's Mot. to Quash ("Opp'n")) at 1. Defendant served Microsoft with a subpoena *duces tecum* pursuant to Federal Rule of Criminal Procedure 17(c) on February 23, 2023. Mot. at 4; Docket No. 73-1 Ex. A. The subpoena contains eleven requests, of which two are now at issue: Request 5 and Request 10. Mot. at 4.

The Requests concern documents that Defendant hopes to use in a motion to suppress. Opp'n at 1. Defendant's motion to suppress will likely focus on whether law enforcement's search of four images of suspected child pornography was justified by the private search exception to the Fourth Amendment or if it improperly exceeded the scope of Microsoft's antecedent review of the images. *Id.* at 3, 11. "[T]he Fourth Amendment protects individuals from government actors, not private ones, [and so] a private party may conduct a search that would be unconstitutional if conducted by the government." *United States v. Wilson*, 13 F.4th 961, 967 (9th Cir. 2021) (internal citation omitted). Under the exception, governmental searches that are coextensive to antecedent private searches are constitutional; governmental searches that exceed antecedent private searches are unconstitutional. *See id.* at 967-71 (discussing the private search exception); *United States v. Jacobsen*, 466 U.S. 109 (1984) (formalizing the private search exception). Defendant thus seeks Microsoft's policies regarding the review of suspected child pornography to determine the nature and scope of Microsoft's alleged manual review in this matter. Opp'n at 3, 11. In particular, Defendant seeks to determine whether Microsoft in fact conducted manual review of each image sent to NCMEC, or whether images were, instead, only screened by automation. *See Wilson*, 13 F.4th at 975 ("[W]hether Google had previously reviewed . . . *other individuals'* files is not pertinent to whether a private search eroded Wilson's expectation of privacy. Under the private search doctrine, the Fourth Amendment remains implicated 'if the authorities use information with respect to which the expectation of privacy has not already been frustrated.'" (quoting *Jacobsen*, 466 U.S. at 117)). Defendant likely hopes that the government's search exceeded Microsoft's search, rendering the private search exception inapplicable, the government's search unconstitutional, and the evidence derived therefrom inadmissible.

Request 5 originally demanded Microsoft produce: "Any training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography, classification standards of suspected child pornography." Docket No. 73-1 Ex. A. Request 10 originally demanded Microsoft produce:

> Any and all policies, procedures, reports, guidelines, manuals, or other materials, regarding the discovery, review, and/or reporting of accounts for suspected child pornography by Microsoft, whether manual or automated; a description of any technology or methods used to search user data, including PhotoDNA[1] and/or similar technologies or methods; and, any communications with employees regarding user/subscriber content to be flagged.

Id.

After negotiations between Microsoft and Defendant, Defendant modified Request 5 to demand:

> The training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography files, and classification standards of suspected child pornography in effect around the time of CyberTip 52016239, from July 5, 2019, [suspected CP first flagged] until August 7, 2019 [date when NCMEC processed the CyberTip].

Mot. at 6. Defendant also modified Request 10 to demand, in part:

> The policies, reports, guidelines, and manuals that set forth the

[1] "PhotoDNA is an image-matching technology . . . that helps Microsoft find and remove images of child sexual exploitation and abuse imagery from its online services." Mot. at 2. It creates a unique digital identifier, or "hash" for images it scans that it compares against the hashes of previously identified images of child sexual exploitation and abuse. *Id.*

> procedures for review, and reporting of accounts containing suspected child pornography files, whether manual or automated . . . from July 5, 2019, [suspected CP first scanned] until August 7, 2019 [NCMEC date processed].[2]

Id. Microsoft has provided "a declaration from a Microsoft employee describing, among other things, the process by which Microsoft reviews suspected images of child sexual exploitation and abuse on its services before reporting them to NCMEC," as well as a data log showing that the images were, in fact, manually reviewed. *Id.* at 6, 15; Docket No. 86 (Microsoft's Suppl. Submission ("Submission")) at 2; Submission Exs. 1, A.[3] Microsoft now moves to quash Request 5 and the above section of Request 10 as insufficiently specific, irrelevant, inadmissible, and unduly burdensome. Mot. at 7-16.

III. <u>LEGAL STANDARD</u>

Federal Rule of Criminal Procedure 17(c) governs the issuance of subpoenas *duces tecum* in federal criminal proceedings. *United States v. Nixon*, 418 U.S. 683, 697-98 (1974). Rule 17(c) provides that:

> A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

Fed. R. Crim. P. 17(c)(1). Rule 17(c) is "not intended as a discovery device." *United States v. Reed*, 726 F.2d 570, 577 (9th Cir. 1984). Instead, its purpose is to provide an opportunity for relevant evidentiary documents to be inspected prior to trial. *See Nixon*, 418 U.S. at 699 n.11. Accordingly, the party seeking evidence under Rule 17(c) bears the burden of "clear[ing] three hurdles: (1) relevancy; (2) admissibility; [and] (3) specificity." *Id.* at 700; *see also United States v. Nosal*, 2013 WL 11327121, at *11–12 (N.D. Cal. Mar. 29, 2013) (Chen, J.) (quoting *Nixon*).

Even if the party that issued the subpoena meets each of these requirements, the court may quash the subpoena "if compliance would be unreasonable or oppressive." Fed. R. Crim. P.

[2] Microsoft only moves to quash the part of Request 10 that is quoted here. Mot. at 16.

[3] Defendant rejected Microsoft's offer to provide this declaration. Mot. at 6. Nevertheless, Microsoft submitted it after oral argument at the Court's direction.

17(c)(2). These requirements apply to subpoenas against third parties. *See United States v. Fields*, 663 F.2d 880, 881 (9th Cir. 1981) ("[W]e see no basis for using a lesser evidentiary standard merely because production is sought from a third party rather than from the United States."). The burden rests on Defendant, as the subpoena's proponent, to prove that the material sought satisfies these criteria. *See United States v. Reyes*, 239 F.R.D. 591, 599 (N.D. Cal. 2006) (holding, in the context of ruling on motions to quash, that "the proponent of a subpoena bears the burden of proving that the information sought is relevant, specific, and admissible"). Ultimately, "[i]t is up to the discretion of the trial court to determine whether a Rule 17(c) subpoena application has met the *Nixon* requirements." *United States v. Pac. Gas & Elec. Co.*, No. 14-CR-00175-TEH-1 (MEJ), 2016 WL 1212091, at *3 (N.D. Cal. Mar. 28, 2016).

IV. DISCUSSION

Microsoft moves to quash Request 5 in full and Request 10 in part as insufficiently specific, irrelevant, inadmissible, unduly burdensome, and cumulative. Because the information Defendant seeks is irrelevant and cumulative of the information Microsoft provides in its supplemental submission (and thus unduly burdensome), the Court quashes Defendant's subpoena.

Defendant seeks documents concerning Microsoft's procedures for reviewing child sex abuse imagery. As noted above, Defendant seeks this information to determine if the private search exception to the Fourth Amendment justified law enforcement's search of four images of suspected child sex abuse, or if the search improperly exceeded the scope of Microsoft's antecedent review. *Id.* at 3, 11. That issue turns on whether Microsoft conducted a manual review of each image. Microsoft, however, has produced sufficient documents concerning the scope of their employees' review of the child sex abuse images at issue.

Microsoft produced the CyberTip to NCMEC in which there is a "Yes" answer next to the question "Did reporting [Electronic Service Provider] view entire contents of the uploaded file?" Docket No. 73-1 Ex. C, at 3-4. Microsoft also submitted the declaration of Alon Brown, the Partner Director of the Digital Trust and Safety Team at Microsoft, in which Mr. Brown explains Microsoft's review process. Submission Ex. 1, ¶ 1. Mr. Brown states that the "Yes" answer is automatically generated and signifies "that someone at Microsoft *visually* reviewed the images at issue before they were sent to NCMEC." *Id.* ¶¶ 11-12 (emphasis added). Additionally, Mr. Brown explains that images are reviewed in one of two ways, depending on if the image's hash matches a verified or unverified hash "provided by a Microsoft-approved source." *Id.* ¶ 9. If the hash matches a verified hash, the image "undergoes a 'confirm review' in which the image and the previously verified classification is shown to an analyst for a single, eyes-on review to confirm if the existing classification correctly reflects the content of the image." *Id.* If the hash is unverified, the image undergoes a "double-blind review" in which the image is independently viewed and analyzed by two employees. *Id.* If the two employees disagree, two or more additional employees and the team management make a final determination. *Id.* "If the content is verified as an image of child sexual abuse, thereafter the image's hash becomes a Microsoft Verified Hash." *Id.* Under both processes, "analysts are instructed to visually inspect every image they are sent to review." *Id.*

Crucially, Microsoft has also produced a log confirming that the four images at issue went through these processes and were manually reviewed. *See id.*, Ex. B. The log confirms when employees submitted their classification decisions, that two of the four images went through the double-blind review process, that the other two went through confirm review process, and that, for each image, the review "process" was "manual." *Id.* Mr. Brown further confirmed that employees visually reviewed the images by "examin[ing] data extracted from logs created by the tool used [by employees] to perform these reviews." *Id.* ¶ 15. Through this examination, he concluded that the images were viewed by analysts in "six unique sessions," the two single review sessions and four double-blind review session (each double-blind review requires two review sessions, since the image is reviewed twice).

Not only do these documents describe Microsoft's review process generally, they also describe the process whereby Microsoft reviewed the four images specific to this matter. This is the information Defendant seeks in Requests 5 and 10, except that the information Microsoft provides is more detailed, since Defendant only seeks Microsoft's general review procedures. The data log, CyberTip, and Mr. Brown's declaration are more than sufficient to determine the scope of Microsoft's review. *See United States v. Bohannon*, 2023 WL 2347420, at *1 (N.D. Cal. Mar. 2, 2023) (concluding, based on the language in a CyberTip and two declarations from Microsoft employees, "that a Microsoft employee reviewed the image at issue . . . before the file was forwarded to NCMEC"); *United States v. Eley*, No. 3:21-cr-00011-MMD-WGC-1, 2022 WL 181255, at *4 (D. Nev. Jan. 20, 2022) (noting, in response to the language in a CyberTip,[4] that the detective who conducted the government's search "could reasonably infer from that unambiguous [CyberTip] statement that a Google employee viewed the entire file"); *United States v. Bonds*, No. 5:21-CR-00043-KDB-DCK, 2021 WL 4782270, at *4 (W.D.N.C. Oct. 13, 2021) (similar).

Since Microsoft has provided enough information to determine the scope of its employees' review, Microsoft's general review procedures are unnecessary and have little, if any, probative value. Defendant's motion to suppress will turn on specific conduct, not general policy. There is no reason to doubt the specific and direct evidence of Microsoft's review of the images, especially when backed by logs. *See Dow Chem. Co. v. United States*, 476 U.S. 227, 239 n.5 (1986) ("Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations."); *Wilson*, 13 F.4th at 968 ("[A]n antecedent private search excuses the government from obtaining a warrant to repeat the search but only when the government search does not exceed the scope of the private one."). Even if the general review procedures were relevant, Mr. Brown discussed these procedures as well in his declaration. The information Defendant now seeks is cumulative and unduly burdensome.[5] *See United States v. Nosal*, 291

[4] The CyberTip at issue explained: "'With respect to the portion of this CyberTip containing the heading: "Was File Reviewed by Company?", when Google responds "Yes" it means the contents of the file reported were viewed by a person concurrently to or immediately preceding the sending of the CyberTip.'" *Eley*, 2022 WL 181255, at *1 (quoting the CyberTip at issues).

[5] The evidence sought by Request 5 is likely inadmissible or duplicative. Request 5 seeks "training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography . . . ." Mot. at 6. Defendant claims to seek these materials "because they are probative of what Microsoft employees do or don't do as part of their CyberTip reporting responsibilities." Opp'n at 11. First, it is unclear how training materials on the definition of child pornography are relevant here, where the issue is the type of review Microsoft conducted, not whether its employees properly flagged the images on a substantive basis. Second, the request for training materials on company reporting procedures is duplicative of Request 10, which already seeks guidelines for reporting procedures. Request 5 is thus inadmissible and cumulative.

F.R.D. 403, 406, 411 (N.D. Cal. 2013*), objections sustained in part and overruled in part*, No. CR-08-0237 EMC, 2013 WL 11327121 (N.D. Cal. Mar. 29, 2013) (noting disapprovingly that "many [of defendant's] requests are duplicative" and that requiring a party to reproduce material is burdensome); *United States v. Ail*, No. CR 05-325-RE, 2007 WL 1229415, at *6 (D. Or. Apr. 24, 2007) ("Further disclosure related to the informants' alleged profits would be cumulative, and defendants cannot use Rule 17(c) as a discovery tool, or a means to conduct a 'fishing expedition.'"); *United States v. Mason*, No. CR 05-324-RE, 2008 WL 1909115, at *2 (D. Or. Apr. 25, 2008) (quashing Rule 17(c) subpoena where "*additional* evidence of [relevant subject] would be cumulative"); *cf. United States v. Weischedel*, 201 F.3d 1250, 1255 (9th Cir. 2000) ("A district court can properly deny a Rule 17(b*)* subpoena request when the testimony sought would be cumulative.").[6]

V. CONCLUSION

For the foregoing reasons, Requests 5 and 10 are irrelevant and unduly burdensome. The Court hereby **GRANTS** Microsoft's motion to quash Request 5 and part of Request 10.

This order disposes of Docket No. 73.

IT IS SO ORDERED.

Dated: June 2, 2023

EDWARD M. CHEN
United States District Judge

[6] Defendant made the Requests in part based on Microsoft's counsel's statements that, aside from information within the CyberTip, Microsoft does "not have records identifying the individual who conducted the manual review of the images at issue in this case, nor the time or place of such review." Opp'n at 3, 5; Docket No. 73-1 ¶ 1 (Crowley declaration); *see also* Docket No. 87-1 Ex. A, at 1 (stating, in an email from Microsoft's counsel to Defendant's counsel, that "Microsoft does not retain specific 'who what when' records on the review of any given image"). In its most recent submission to the Court, Microsoft demonstrates that it does in fact, perhaps unbeknownst to its own counsel, keep records relating to specific reviews, including the "when" of when reviewers submitted their classifications to NCMEC. Submission Ex. 1 ¶ 16.